

**Roger Williams University**  
**DOCS@RWU**

---

Law Faculty Scholarship

Law Faculty Scholarship

---

5-14-2015

# Clapper and the Costs of Overlooking Use Restrictions

Peter Margulies

*Roger Williams University School of Law*

Follow this and additional works at: [https://docs.rwu.edu/law\\_fac\\_fs](https://docs.rwu.edu/law_fac_fs)



Part of the [Immigration Law Commons](#)

---

## Recommended Citation

Peter Margulies, Clapper and the Costs of Overlooking Use Restrictions, Lawfare (May 14, 2015, 2:55 PM), <https://www.lawfareblog.com/clapper-and-costs-overlooking-use-restrictions>

This Article is brought to you for free and open access by the Law Faculty Scholarship at DOCS@RWU. It has been accepted for inclusion in Law Faculty Scholarship by an authorized administrator of DOCS@RWU. For more information, please contact [mwu@rwu.edu](mailto:mwu@rwu.edu).

# Clapper and the Costs of Overlooking Use Restrictions

By **Peter Margulies** Thursday, May 14, 2015, 2:55 PM

## Privacy Paradox: Rethinking Solitude

The Second Circuit’s decision in *ACLU v. Clapper* holding that the section 215 metadata program exceeds statutory authorization has flaws, including this: The ruling focuses on initial collection exclusively, and thus fails to reckon properly with the tight restrictions imposed on government analysts’ access to and use of metadata.

It may seem counter-intuitive to look at data use to decide whether the data is relevant for collection purposes in the first instance. But use, in fact, really matters to relevance. To understand why, it’s useful to refer to section 215’s text, which permits a court to require production of information that is “relevant to an authorized investigation.” The meaning of relevance under section 215 is central, as the *Clapper* court rightly noted. The government, along with Judge Pauley of the Southern District of New York and numerous judges on the Foreign Intelligence Surveillance Court (FISC), asserted that relevance under section 215 was functional in nature: if information requested by the government would assist counterterrorism officials in finding links between individuals and entities that would otherwise elude detection, that information would meet the statutory standard. Analysis of metadata, Judge Pauley opined, allows more thorough investigation of patterns that can reveal previously unknown links. Judge Pauley noted that the comprehensive database of call records that the government had obtained under section 215 facilitated more targeted queries. Because the National Security Agency (NSA) had control of the database, the inquiry could be more comprehensive than would be possible if private firms with divergent data platforms retained possession of the data. Moreover, the NSA’s retention of the data, according to Judge Pauley, allowed the government to pose a targeted query instantaneously, without the delays engendered by seeking a separate court order for an array of private firms.

This functional definition stems from dictionary definitions of the term, “relevant,” which include flexible connotations such as “bearing on... the matter at hand” (OED). Moreover, the Second Circuit has repeatedly cautioned that judicial review under the Foreign Intelligence Surveillance Act (FISA) requires a measure of deference to official requests. As the Second Circuit said in the landmark 1984 FISA case, *United States v. Duggan*, courts should subject government requests to no more than “minimal scrutiny,” taking care not to “second-guess the executive branch.”

Under this functional definition of relevance, the broad collection of metadata and the FISC’s restrictions on analysts’ access to the data are a package deal. Both the FISC and Judge Pauley agreed that counterterrorism officials’ targeted queries of the database were vital to their assessment that the program met the statutory standard. A functional approach would not have allowed the government to gain unfettered access to the data it collected, since such a roving license would have exceeded the targeted criteria that the FISC and Judge Pauley agreed were vital. Unfettered access would have allowed the indiscriminate incursions on privacy that critics of the metadata program fear. To preclude this dystopian result, the FISC tightly regulated such access, among other things permitting only those queries based on “reasonable and articulable suspicion” (RAS) of terrorist ties.

Since 2009, the FISC has approved all RAS identifiers, including phone numbers, which consisted of several hundred carefully tailored data points. Any other queries were off-limits. Much of the concern engendered by the metadata program boils down to worries that analysts could evade the use restrictions. However, dogged reporters searching for post-2009 evidence of such abuse have uncovered only isolated and idiosyncratic violations of the RAS standard. That compliance with judicially-imposed access restrictions is a far cry from the wholesale intrusions recounted by the 1970s Church Committee and invoked by Judge Gerard Lynch, who wrote for the *Clapper* panel.

Judge Lynch read relevance more narrowly than Judge Pauley or the FISC. He declined to accord the government the deference that the Second Circuit had displayed in *Duggan* and its progeny. Instead of a functional approach keyed to the government’s counterterrorism mission, Judge Lynch relied on a recipient-based approach to the relevance of the government’s requests. On this recipient-based view, the government could seek the “records of a particular individual or corporation under investigation,” but not exceed those parameters. Applying this view, the government’s collection of most land-line call records exceeds the relevance standard. Use restrictions that governed post-collection official conduct are irrelevant. Probably for this reason, Judge Lynch’s legal analysis did not mention the FISC’s use restrictions, although the court mentioned use restrictions in its statement of facts.

If *Clapper* had concerned a discovery dispute in a civil lawsuit or a government request in a routine criminal investigation, its analysis would be sound. The intuitive rightness of Judge Lynch’s approach for these prosaic settings probably accounts for much of the wide approval it has elicited. However, that mundane milieu is *not* the appropriate backdrop for assessing relevance under section 215. As noted above, the Second Circuit has applied a far more deferential approach in the context of national surveillance. Under a deferential approach, a plausible argument by the government should prevail, even if a reviewing court feels that its own approach is more intuitively correct. If the Second Circuit’s warning about not second-guessing the executive branch on national security surveillance means anything, it means that the court cannot substitute its judgment

for a plausible judgment made by executive branch officials. Unfortunately, Judge Lynch did not explain why this deferential approach was inapplicable under section 215, which Congress enacted to grant the government what Senator Kyl called the “agility” to anticipate and deter terrorist threats.

In the more deferential national security setting, analyzing section 215 collection without reference to use restrictions is a bit like producing Shakespeare’s Hamlet without an actor to play the Prince of Denmark. In Hamlet, the prince’s scruples make the play; so, too, with section 215’s restrictions on who gets to see and analyze the metadata. Without analysis of those restrictions, the metadata program seems like a disproportionate data grab without adequate statutory authorization---an attempt to “hide elephants in mouseholes,” as Judge Lynch (quoting the Supreme Court) put it. Factor in the downstream rules for querying and analyzing, and the metadata program looks more like a reasonable, proportionate response to the dynamic nature of terrorist threats.

A more careful opinion might have acknowledged the role of such restrictions, and then taken them on directly--- by explicitly finding them insufficient or beside the point. I suppose the opinion’s collection-focused analysis might be said to *imply* such an approach; still, the *Clapper* court made no mention of a mission-critical feature of the program. That made the decision unfaithful to the actual practices that the Second Circuit purported to review, and inconsistent with the deference the Second Circuit has historically shown in national security cases.

Consider the appeals court’s discussion of the metadata program and FBI threat assessments. The Second Circuit reasoned that because the latter (which require at least some threshold showing before the government may proceed) are explicitly carved out of Section 215’s coverage, then the call records program (which involves comprehensive collection of telephony metadata *before* any nexus between the collected stuff and a particular threat, or even a need to examine the data itself, arises) couldn’t possibly be kosher, either.

This is precisely where use restrictions ought to matter---or should have, anyway. As the Second Circuit observed, threat assessments may be undertaken liberally, almost on the government’s own initiative---they require no factual predication at all. Only a few gentle strictures apply: According to one example described in an FBI operations guide (and also cited by the *Clapper* court), an assessment may go forward when there is a reason to collect information, in order determine whether a threat exists; there must also be a rational relationship between the assessment’s purpose, the sought information, and the means chosen to attain it. But only inquiries “pursued for frivolous or improper purposes,” or based on “arbitrary or groundless speculation,” are clearly out of bounds. Such criteria are loose, to say the least. And, more importantly, they do *not remotely resemble the tight limits imposed on the metadata program by the FISC’s RAS mandate*. Congress could (and did) bar collection under section 215 for purposes of a threat assessment. But Congress’s mere mention of threat assessments says little or nothing about its view of the program that the FISC actually authorized---and *that* is what the *Clapper* plaintiffs challenged as incompatible with the statute.

Ultimately, the ruling may further the cause for reforms, like those in the USA Freedom Act, that address fears about collection and preserve government’s necessary capabilities. Moving collection to the private sector and establishing some independent voice to oppose the government’s FISC requests will bolster the program’s legitimacy. However, support for reforms need not obscure the restrictions in place on the current metadata program. The *Clapper* court failed to reckon with those restrictions, although the Second Circuit’s deferential approach to national security surveillance required that reckoning. Perhaps the Second Circuit was wrong to opt for deference in earlier cases, but respect for precedent required some explanation from the *Clapper* court of the errors in the prior approach. Despite the superficial plausibility of its analysis, the court’s failure to provide that explanation makes *Clapper* a flawed decision.

**Topics: Surveillance, FISA, FISA: 215 Collection, FISA: Reform**

---

Peter Margulies is a professor at Roger Williams University School of Law, where he teaches Immigration Law, National Security Law and Professional Responsibility. He is the author of *Law’s Detour: Justice Displaced in the Bush Administration* (New York: NYU Press, 2010).